

Internet Censorship in India: Peeking Under the Hood

Devdutta Mukhopadhyay

Global Network Initiative-Internews Fellowship 2020
Associate Litigation Counsel, Internet Freedom Foundation

I. Introduction and Background

For policy researchers interested in studying internet access and usage, India represents a paradox where price barriers are low but government ordered internet restrictions are rampant. In 2019, India had the cheapest mobile internet prices anywhere in the world¹ but it was also responsible for 121 out of 213 documented internet shutdowns imposed globally.² Largely driven by low prices, internet penetration in India has increased from 8% of the population in 2011 to 55% in 2020.³ The co-existence of these phenomena may appear strange at first glance but it is consistent with previous research which has found that government ordered network disruptions may be more likely in countries which are experiencing rapid expansion in internet connectivity, at least until a tipping point is reached.⁴

As the internet becomes an indispensable fixture in the lives of ordinary Indian citizens, it has also amplified pre-existing societal fault lines. It is, therefore, no surprise that state governments have frequently resorted to network disruptions by invoking national security or public order concerns to suppress real world protests. More curiously, network disruptions have also been ordered for reasons which seem absurdly trivial in comparison such as preventing cheating in school examinations.⁵ While such instances are less common, they provide valuable insight into how easily the extraordinary power to deprive an entire population of internet access can be abused by misguided government officials within the existing legal and institutional framework.

¹ Prasanto K Roy, 'Mobile Data: Why India has the World's Cheapest' BBC (18 March 2019). Available at: <https://www.bbc.com/news/world-asia-india-47537201>

² Berhan Taye, 'Targeted, Cut Off and Left in the Dark: The #KeepItOn Report on Internet Shutdowns in 2019' Access Now (2020). Available at: <https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf>

³ Telecom Regulatory Authority of India, 'The Indian Telecom Services Performance Indicators, January-March 2020'. Available at: https://www.trai.gov.in/sites/default/files/PIR_17092020_0.pdf ; Internet and Mobile Association of India, 'Report on Internet in India (I-Cube) 2011.' Available at: <https://cms.iamai.in/Content/ResearchPapers/bf0de542-aeed-46b3-85e0-9d7ea329fc1c.pdf>

⁴ Jan Rydzak, 'Disconnected: A Human Rights Based Approach to Network Disruptions' Global Network Initiative (2018). Available at: <https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf>

⁵ The Telegraph, 'Net Curbs in 7 districts for Madhyamik' (17 February 2020). Available at: <https://www.telegraphindia.com/west-bengal/net-curb-in-7-districts-for-madhyamik/cid/1746162>

As researchers have previously argued, it is useful to think about network disruptions as a spectrum.⁶ For the purposes of this policy brief, we have drawn from the case studies discussed in the later sections and defined an internet shutdown as an *intentional* disruption ordered by a *government actor* which denies the population of a region *effective access* to (a) the internet in its entirety (*conventional shutdowns*), or (b) denial of access to a class of websites (*blacklisting*, e.g. social media bans), or (c) selective access to only a class of websites (*whitelisting*). Further, the dual nature of the internet as a communication medium and essential infrastructure will be central to our analysis of the impact of internet shutdowns. This is especially relevant during the COVID-19 pandemic which has led to online modes of service delivery substituting their physical analogues.

While internet shutdowns are the most draconian tool used to control the flow of information, Indian internet users have also experienced an increase in blocking of specific websites and mobile apps. On 29 June 2020, in what was termed by many government supporters as a ‘digital surgical strike,’ India banned 59 Chinese-origin mobile apps including Tik Tok and We Chat.⁷ This overnight ban was the first of its kind in the world and it refocused attention on India’s opaque and unaccountable website blocking process which was held to be constitutional by the Supreme Court of India in 2015.⁸ At first glance, the process prescribed for website blocking under Section 69A of the Information Technology Act, 2000 seems to adhere to requirements of due process since a website owner must be provided a pre-decisional hearing and the competent authorities are required to issue a written order containing reasons for blocking a website. These considerations weighed heavily on the Supreme Court’s mind while adjudicating the constitutionality of Section 69A, and the Court concluded that if the final decision of the government authorities was incorrect, it could always be challenged before a High Court by filing a writ petition.

However, recent experience has shown that the Supreme Court’s faith in adherence to procedure by government authorities may have been misplaced. As the case studies discussed in the later sections will show, in reality, website owners are often not provided any pre-decisional hearing and they may even be denied access to website blocking orders. For many individuals and organizations who have faced website blocking, even finding out if their website has been rendered inaccessible due to a technical error or a government order is a significant challenge. As researchers at the Centre for Internet & Society have found,

⁶ Eleanor Marchant and Nicole Stremlau, ‘A Spectrum of Shutdowns: Reframing Internet Shutdowns from Africa’ *International Journal of Communication* 14 (2020), pg. 4327-4342.

⁷ Press Information Bureau, Government of India, ‘Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order’ (29 June 2020). Available at: <https://pib.gov.in/PressReleaseDetailm.aspx?PRID=1635206>

⁸ Shreya Singhal v. Union of India (2015 5 SCC 1). See also Devdutta Mukhopadhyay, ‘Shreya Singhal v. Union of India’s Blindspot: Website Blocking’ *Live Law* (28 March 2020). Available at: <https://www.livelaw.in/columns/shreya-singhal-v-union-of-indias-blindspot-website-blocking-154451>

website blocking is inconsistently implemented by different Internet Service Providers (ISPs) and only 27.64% of the websites included in their sample were uniformly blocked by all six major Indian ISPs.⁹ Such inconsistent website blocking by ISPs adds to the confusion and makes it difficult to determine the true cause of a website being inaccessible. In some cases, website owners are informed by ISPs or domain registrars that their website has been blocked pursuant to a government order but obtaining a copy of the order is another uphill battle since website blocking orders are treated as confidential under existing law.¹⁰

In this policy brief, we will study internet shutdowns and website blocking in India by focusing on orders issued by government authorities to impose these restrictions. This methodological choice is motivated by lack of existing literature which analyses the legal orders through which internet censorship is implemented. These legal orders and their content occupy a central role in litigation challenging internet shutdowns or website blocking, and they also determine the leeway available to ICT companies to narrowly interpret the scope of restrictions. Most importantly, these legal orders provide us insight into the material available with government officials at the time of censorship being authorized and must be capable of surviving legal scrutiny on their own without further explanations or justifications being required later in time. As the Indian Supreme Court has famously noted, *“Orders are not like old wine becoming better as they grow older¹¹.”*

We have structured our analysis of the legal orders authorizing internet shutdowns and website blocking in the form of case studies. Our first set of case studies will analyse internet shutdown orders issued by government authorities in the states of Jammu & Kashmir, Rajasthan and Bihar to understand the factual circumstances prompting internet shutdowns, the type of services affected, the geographic and temporal scope of internet shutdowns, and the role of government officials at different levels of the administrative hierarchy. Our second set of case studies will look at two instances of website blocking faced by the creator of a satirical website and a group of environmental campaigners to demonstrate the arbitrary and opaque nature of website blocking in India. Based on these case studies, we will develop recommendations for lawyers, civil society organizations and private companies which explain how different stakeholders can help mitigate the negative impact of internet shutdowns and website blocking.

⁹ Kushagra Singh, Gurshabad Grover & Varun Bansal, ‘How India Censors the Web’ Centre for Internet & Society (17 January 2020). Available at: <https://cis-india.org/internet-governance/blog/how-india-censors-the-web>

¹⁰ Rule 16, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

¹¹ Mohinder Singh Gill v. Chief Election Commissioner (1978 SCR 3 272).

II. Case Studies: Internet Shutdowns

A. Jammu & Kashmir

While internet shutdowns are a pan-India problem, Jammu & Kashmir has borne the brunt of them. In 2019, Jammu & Kashmir accounted for 68% of internet shutdowns imposed in India.¹² More troublingly, on 05 August 2020, internet restrictions which were first imposed at the time of revocation of the erstwhile state's semi-autonomous status under the Constitution crossed their one-year anniversary and rank as the longest internet shutdown imposed by any democratic government.¹³ To add insult to their injury, the residents of Jammu & Kashmir have been expected to pay telecom service providers for services they were not able to use because of government ordered restrictions.¹⁴

When the ongoing internet shutdown in Jammu & Kashmir was first imposed on 05 August 2019, its underlying legal basis was unclear since there were no orders available in the public domain which authorized cutting off all communication channels including landline, phone calls, SMS services, mobile internet and fixed line internet. This complete communication shutdown was challenged before the Supreme Court of India, which in its judgement delivered on 10 January 2020 directed the government to review the internet restrictions in accordance with the principle of proportionality and imposed a mandatory obligation to publish all internet shutdown orders.¹⁵

While the judgement of the Supreme Court in *Anuradha Bhasin v. Union of India* did not offer any immediate substantive relief to the petitioners, it did stir the executive branch into action. Two weeks after the judgement was delivered, the government restored 2G mobile internet and fixed line internet and allowed access a select list of whitelisted websites with a complete ban on social media and virtual private networks (VPNs).¹⁶ However, researchers soon demonstrated that such a whitelisting system was technically infeasible due to the interconnected nature of the internet.¹⁷ In their excellent analysis, Rohini Lakshane and Prateek Waghre analysed the web performance of 301 whitelisted websites and found that

¹² Supra note 2 at pg.19.

¹³ Mitch Prothero, 'India's 134-day long internet shutdown in Kashmir is now the longest ever imposed by a democratic state' Insider (16 December 2019). Available at: <https://www.insider.com/kashmir-internet-shutdown-imposed-india-longest-ever-by-democracy-2019-12>

¹⁴ Sushovan Sircar, 'Kashmiris asked to pay post-paid dues for Aug-Sept blockade' The Quint (14 October 2020). Available at: <https://www.thequint.com/news/india/postpaid-mobile-phone-services-kashmiris-asked-to-clear-post-paid-bills>

¹⁵ *Anuradha Bhasin v. Union of India* (2020 3 SCC 637). See also Devdutta Mukhopadhyay & Apar Gupta, 'Jammu & Kashmir Internet Restriction Cases: A Missed Opportunity to Redefine Fundamental Rights in the Digital Age' Indian Journal of Constitutional Law, Vol. 9 (August 2020). Available at: https://ijcl.nalsar.ac.in/wp-content/uploads/2020/08/9IndianJConstL207_MukhopadhyayGupta.pdf

¹⁶ Home Department, Government of Jammu & Kashmir, Order No. Home- 05 (TSTS) of 2020 dated 24.01.2020. Available at: [http://jkhome.nic.in/Home-05\(tsts\)%20of%202020_0001.pdf](http://jkhome.nic.in/Home-05(tsts)%20of%202020_0001.pdf)

¹⁷ Rohini Lakshane & Prateek Waghre, 'Even the 301 whitelisted sites in Jammu and Kashmir are not entirely accessible: An analysis' Medianama (28 January 2020). Available at: <https://www.medianama.com/rohini-lakshane-prateek-waghre-analysis-of-whitelisted-urls-in-jammu-and-kashmir-january-2020/>

they would be fully functional only if the web application is permitted to make network calls to other websites to load JavaScript, style sheets, maps, videos, images, analytics etc. They further found that in many cases, while the website's main domain had been whitelisted, its subdomains which contained the log in page or other important features remained blocked.

Finally, on 04 March 2020, the whitelisting system was scrapped and the ban of social media and VPNs was lifted.¹⁸ However, mobile internet speed in Jammu & Kashmir continues to be slowed down to 2G till date.¹⁹ At this stage, it is worth noting that the vast majority of residents of Jammu & Kashmir rely on mobile internet services to access the web and do not have fixed line internet connections.²⁰ For people without access to computers and fixed line connections, there is no meaningful internet access due to speed being slowed down to 2G. Theoretical and simulated comparisons of web performance at 2G v. 4G speed indicate that tasks on observed 2G speed can take up to 50 times longer.²¹ 2G network conditions are also well below the minimum requirements of video communication platforms like Zoom and Skype which have become a life line during the COVID-19 pandemic and facilitated access to telemedicine and online education.²² Interviews with residents of Jammu & Kashmir paint a bleaker picture and reveal that even simple tasks such as attaching files to emails or downloading intensive care guidelines cannot not be executed on 2G speed.²³

Since January 2020, the Government of Jammu & Kashmir has issued 102 orders under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 (Telecom Suspension Rules) imposing or modifying restrictions on internet access.²⁴ In compliance with the directions issued in *Anuradha Bhasin v. Union of India*, these orders have been published on an official government website. Out of these, 24 are standard orders issued by the Home Secretary and 78 are emergency orders issued by the Inspector General of Police which were subsequently confirmed by the Home Secretary. While the regular orders prescribe baseline restrictions for the entire union territory of Jammu & Kashmir

¹⁸ Home Department, Government of Jammu & Kashmir, Order No. Home- 17 (TSTS) of 2020 dated 04.03.2020. Available at: [http://jkhome.nic.in/17\(tsts\)20200001.pdf](http://jkhome.nic.in/17(tsts)20200001.pdf)

¹⁹ Home Department, Government of Jammu & Kashmir, Order No. Home- 114 (TSTS) of 2020 dated 21.10.2020. Available at: [http://jkhome.nic.in/114\(TSTS\)of2020.pdf](http://jkhome.nic.in/114(TSTS)of2020.pdf)

²⁰ There are 0.08 million wireline broadband subscribers and 5.82 million wireless broadband subscribers in Jammu & Kashmir. See Ministry of Communications, Government of India, Telecom Statistics India-2019. Available at <https://dot.gov.in/sites/default/files/Telecom%20Statistics%20India-2019.pdf?download=1>

²¹ Prateek Waghre, 'Implication of 4G and 2G connection speeds on web performance' Affidavit filed before the Supreme Court of India in Foundation for Media Professionals v. U.T. of Jammu & Kashmir, Diary No. 10817 of 2020. Available at: <https://drive.google.com/file/d/1kk5WH4NvXv3zcrVGzWmsgFelffQwSA3O>

²² Id

²³ Revati Laul, 'Personal Testimonies from Residents of Jammu & Kashmir' Affidavit filed before the Supreme Court of India in Foundation for Media Professionals v. U.T. of Jammu & Kashmir, Diary No. 10817 of 2020. Available at: <https://drive.google.com/file/d/1M7x7G4QuLfo6w7uqucEEGPj6kIMQDjOR>. See also Jammu & Kashmir Coalition of Civil Society, 'Kashmir's Internet Siege: An Ongoing Assault on Digital Rights' (August 2020). Available at: <https://jkccs.net/report-kashmirs-internet-siege/>

²⁴ Database of internet shutdown orders issued by Government of Jammu & Kashmir. Available at: <https://archive.org/details/india-internet-shutdown-orders-database>

consisting of 20 districts for periods ranging up to 23 days, the emergency orders typically impose additional restrictions in specific districts for periods ranging up to nearly 4 days. The standard orders which now slowdown mobile internet speed to 2G do not provide any reasons which would explain their expansive geographic scope and barring notable exceptions, they do not cite any specific incidents or their location. In contrast, the emergency orders typically reference specific incidents in an area- the most common being encounters between security forces and terrorists - to justify complete suspension of mobile internet services in that particular district and its adjoining districts. Therefore, through the standard orders, 2G speed has been established as the baseline norm which requires little justification, and through the emergency orders, even 2G mobile internet access can be taken away if any actual violence occurs in an area.

Division	Districts/ Areas	Duration (In Hours)
Kashmir	Pulwama/ Awantipora in Pulwama	574.5
	Shopian	439.5
	Kulgam	356
	Anant Nag	246.5
	Baramulla/ Sopore in Baramulla	233
	Srinagar	222
	Kupwara/ Handwara in Kupwara	131.5
	Budgam	127.5
	Bandipora	81
	Ganderbal	81
Jammu	Ramban	24

[Table showing total duration of mobile internet suspension through emergency orders in different districts of Jammu & Kashmir in 2020.]

An analysis of the reasons provided in the orders also fits the trend of most internet shutdowns being proactive rather than reactive in nature. For instance, consider the standard order issued on 04 April 2020 which cited public opposition to amendments to Jammu & Kashmir's domicile laws as one of the reasons which necessitated extension of the internet slowdown across the Union Territory. In addition to this, emergency orders were also issued suspending mobile internet access entirely in districts of Kashmir on occasions like Republic Day and Independence Day, which further demonstrates the pre-planned and almost routine nature of internet shutdowns in the region. In some cases, the orders refer to surrounding circumstances such as encounters between security forces and terrorists, recovery of arms/ammunitions and creation of new terror outfits to suggest a heightened threat level which would justify extension of the internet restrictions. If the intended targets of these internet restrictions are terrorists, their effectiveness is doubtful since terrorist groups often have their own underground communication networks and they can also use regular cellular services or 2G internet to coordinate and plan their attacks. The internet restrictions may

similarly fail at their objective of maintaining public order since empirical studies suggest that internet shutdowns may actually incentivize violent protests which require less communication and coordination than peaceful demonstrations.²⁵ The inability of internet restrictions to prevent large public gatherings is also evident from the standard order issued on 15 April 2020 which notes that despite mobile internet speed being slowed down to 2G, over 500 villagers congregated for the funeral of a militant.

It should be noted that while the vast majority of the orders only impose restrictions on mobile internet access, there have been at least 3 instances of mobile cellular services, which include voice calls and SMS, also being snapped in districts of Kashmir in 2020. For instance, mobile cellular services were suspended in Srinagar for 18 hours on 19 May 2020 and mobile internet services were also suspended for nearly 4 days. To justify the necessity of this communication shutdown, the orders cite an encounter between security forces and terrorists and the likelihood of data services being misused to incite the general public. However, we must remember that such orders only present the government's version of events. For instance, what the orders issued on 19 May 2020 fail to record is the widespread damage caused to homes of civilians and allegations that civilians were used as human shields by the security forces during the encounter in downtown Srinagar.²⁶ Therefore, suspension of internet and other communication channels can easily become a tool to cover up human rights abuses by government actors and any claims made to justify such restrictions must be subjected to the highest level of scrutiny.

B. Rajasthan

With 70 documented internet shutdowns since 2012, the north-western state of Rajasthan has witnessed the second highest number of internet shutdowns in India after Jammu & Kashmir.²⁷ A long-standing problem in Rajasthan has been issuance of internet shutdown orders by Divisional Commissioners who are mid-level bureaucrats lacking authorization under the law to exercise these powers. This issue was also litigated before the Rajasthan High Court when internet shutdown orders were issued to prevent cheating in police constable recruitment exams in July 2018. However, the Court did not decide whether Divisional Commissioners are empowered to impose internet shutdowns under existing law since the government provided an undertaking that it would not impose internet shutdowns to prevent cheating in examinations in the future.²⁸

²⁵ Jan Rydzak, 'Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India' (7 February 2019). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413

²⁶ Junaid Kathju, 'Srinagar Encounters: Houses Burned and Looted, Used as Human Shields Allege Residents' The Wire (21 May 2020). Available at: <https://thewire.in/rights/kashmir-srinagar-encounter>

²⁷ Software Freedom Law Centre, Internet Shutdown Tracker. Available at: <https://internetshutdowns.in/>

²⁸ Internet Freedom Foundation, 'An incremental victory in the Rajasthan HC against Internet Shutdowns #KeepUsOnline' (04 December 2018). Available at: <https://internetfreedom.in/an-incremental-victory-in-the-rajasthan-hc-against-internet-shutdowns/>

We analysed 22 internet shutdown orders issued in Rajasthan from 2017 to 2019 and all of the orders were issued by Divisional Commissioners under Rule 2(1) of the Telecom Suspension Rules.²⁹ The orders indicate that the power to impose internet shutdowns was delegated by the Home Secretary, who is the actual authority mentioned in Rule 2(1), to Divisional Commissioners through a letter issued on 02 September 2017. While delegation of powers is permissible under Rule 2(1) for emergency situations, any orders issued by the delegate must be confirmed by the Home Secretary within 24 hours and the delegate must not be below the level of a Joint Secretary. However, the orders supplied by the Rajasthan Government in response to our Right to Information request do not contain any orders issued by the Home Secretary which approve the orders issued by Divisional Commissioners. This practice of delegating the power to impose internet shutdowns to mid-level bureaucrats has also been discouraged by the central government which noted that frequent disruptions were being imposed by Divisional Commissioners in Rajasthan and urged the state government to reconsider its stance and ensure strict compliance with the law.³⁰

On a more positive note, the orders issued by the Rajasthan Government reveal that the internet shutdowns are relatively narrow in their geographic scope and 17 out of 22 orders were clearly limited to specific areas within a district rather than the district in its entirety. For instance, the internet shutdown orders which were issued in July 2018 to prevent cheating in police constable recruitment examinations actually list specific addresses of examination centres across five districts where internet services had to be suspended. However, since there were 350 examination centres and internet services had to be suspended within a 5 km radius of all centres, the impact of the restrictions was widespread and could be classified as an internet shutdown.³¹ It should be noted that nearly 15 lakh candidates were scheduled to appear in the police constable recruitment exam and the exam had already been cancelled once after the police caught a hi-tech gang involved in facilitating cheating by candidates. In these circumstances, the actions of the government officials seem well-intentioned but they failed to recognize that an internet shutdown was not necessary because such problems can be addressed through less restrictive measures such as better invigilation, use of CCTV cameras and localized signal jammers.

The relatively narrow geographic scope of the internet shutdowns can also be attributed to the localized nature of law and order disturbances that they seek to address. Some of the longest internet shutdowns imposed by government authorities in Rajasthan have been in response to public protests against actions of local government officials and incidents of crime

²⁹ Database of internet shutdown orders issued by Government of Rajasthan. Available at: <https://archive.org/details/india-internet-shutdown-orders-database>

³⁰ Department of Telecom, Government of India, Letter to Government of Rajasthan dated 28.09.2018. Available at: <https://archive.org/details/do-t-letter-to-rajasthan-govt>

³¹ Deccan Chronicle, 'Internet to be shut during constable recruitment exams in Rajasthan' (12 July 2018). Available at: <https://www.deccanchronicle.com/nation/current-affairs/120718/internet-to-be-shut-during-constable-recruitment-examinations-in-rajas.html>

which have led to mobilization along lines of religion or caste. For instance, an almost 5 day long internet shutdown was imposed in parts of Jaipur on 09 September 2017 after violent clashes broke out between the police and protestors who had gathered to demand action in an incident of police brutality.³² Mobile internet services were again suspended for nearly 4 days in Jaipur from 02 July 2019 after agitations against the rape of a 7 year old child took a communal turn through spreading of rumours on social media.³³

Finally, the orders reveal that the nature of services affected by internet shutdowns in Rajasthan has also changed over the years. While the initial orders directed suspension of all internet services, the orders issued after mid-2018 specifically exempt broadband or fixed line internet services. The orders also direct blocking of social media platforms like WhatsApp, Facebook and Twitter but it is unclear if service providers were expected to block these websites for fixed line connections in addition to suspending mobile internet services in their entirety.

C. Bihar

By analysing 30 orders issued by the Home Secretary, Government of Bihar under the Telecom Suspension Rules in 2017 and 2018, we learnt that the Rules which were meant to authorize conventional internet shutdowns were actually being used by the state government to block access to specific mass messaging platforms such as Facebook, Twitter and WhatsApp.³⁴ Blocking of websites and mobile applications should typically take place under Section 69A of the Information Technology Act, 2000 but the fact that powers under Section 69A are only available with the central government may have motivated the state government of Bihar to use the Telecom Suspension Rules for this purpose.

While the orders themselves are extremely vague and do not cite any specific incidents which prompted their issuance, contemporaneous media reports suggest that most social media bans imposed in Bihar were in response to communal clashes erupting after events like desecration of religious idols,³⁵ discovery of cow carcasses³⁶ and during religious

³² Akriti Paracer, '1 dead in clash between locals and police in Jaipur, curfew imposed' The Quint (09 September 2017). Available at: <https://www.thequint.com/news/india/jaipur-ramganj-violence-curfew>

³³ Rajesh Asnani, 'Rape of 7-year old girl creates unrest in Jaipur, police shut down internet to prevent spreading of rumors' New Indian Express (02 July 2020). Available at: <https://www.newindianexpress.com/nation/2019/jul/02/rape-of-7-year-old-girl-creates-unrest-in-jaipur-police-shut-down-internet-to-prevent-spreading-of-1998485.html>

³⁴ Database of internet shutdown orders issued by Government of Bihar. Available at: <https://archive.org/details/india-internet-shutdown-orders-database>

³⁵ News 18 India, 'Nawada Becomes 8th District in Bihar facing Communal Violence, Internet Services Suspended' (30 March 2018). Available at: <https://www.news18.com/news/india/idol-vandalised-in-bihars-nawada-sparks-communal-violence-again-1703689.html>

³⁶ Ruchir Kumar & Aditya Nath Jha, 'Internet services suspended in 7 districts in Bihar after carcasses found floating in canal' Hindustan Times (05 September 2017). Available at: <https://www.hindustantimes.com/india-news/internet-services-suspended-in-7-districts-of-bihar-after-carcasses-found-floating-in-canal/story-QI1kptjbOc4fMA7gpeofwJ.html>

processions.³⁷ To provide a historical perspective to the Bihar government's social media bans, we must note that the eastern state has witnessed one of the worst communal riots in the history of India with over 1000 people being killed and 50,000 people being displaced during the Bhagalpur riots of 1989.³⁸

The duration of social media bans in Bihar is fairly prolonged with single orders authorizing up to 4 days of restrictions in cases where communal clashes spill over to other districts and continue over several days. However, with respect to the range of services affected, the orders were relatively narrow and only directed blocking of mass messaging platforms while clearly exempting banking, railways and other government services. Another interesting way in which the Bihar government tried to narrow the scope of restrictions was by prohibiting only new uploads on YouTube while allowing people to watch existing videos.

III. Case Studies: Website Blocking

A. Blocking of satirical website, Dowry Calculator

In 2011, journalist and film critic, Tanul Thakur created a satirical website called Dowry Calculator to mock the patriarchal social practice of dowry. He dedicated the website to "*all the match-making aunties of India*" and created a quiz which would determine how much dowry a groom could expect based on attributes which are traditionally considered valuable in Indian society such as caste, skin colour, height, educational qualifications etc. The satirical intent of the website was evident from the options provided to users and the phrasing of the final results. The dark humour struck a chord with many young Indians and Dowry Calculator was featured positively by several media outlets.³⁹

Around September 2018, more than 7 years after its launch in 2011, Dowry Calculator was suddenly blocked after it became the subject of controversy on social media. A few months prior to blocking of the website, two prominent politicians had criticized Dowry Calculator on Twitter and demanded action against it. However, since the website had only been blocked by certain ISPs and remained accessible through other ISPs, it was not immediately clear if it was an instance of government ordered blocking. To obtain greater clarity, a Right to Information request was filed by the website owner with the Ministry of Electronics &

³⁷ New Indian Express, 'Bihar communal violence: Two BJP leaders held' (29 March 2018). Available at: <https://www.newindianexpress.com/nation/2018/mar/29/bihar-communal-violence-two-bjp-leaders-held-1794291.html>

³⁸ Hindustan Times, 'Chronology of Communal Violence in India' (09 November 2011). Available at: <https://www.hindustantimes.com/india/chronology-of-communal-violence-in-india/story-jJtcgvxFYh5N3jhSw7H4KN.html>

³⁹ Sneha Mahale, 'Satire app gets 5 lakh hits in a month' Hindustan Times (16 June 2011). Available at: <https://www.hindustantimes.com/india/satire-app-on-dowry-gets-5-lakh-hits-in-a-month/story-q8toyg4uzE961zo0Tj2RKO.html> ; Sita Wadhwani, 'Dowry Calculator app: How much for an arranged marriage?' CNN Travel (02 June 2011). Available at: <http://travel.cnn.com/mumbai/life/ behold-dowry-calculator-872055/>

Information Technology seeking a copy of the website blocking order. The response received from the government stated that Dowry Calculator had been blocked because *“its content was illegal and it portrayed the country in a poor light.”* The government also declined to share a copy of the website blocking order by citing the confidentiality requirement present under India’s website blocking law.

The blocking of Dowry Calculator was eventually challenged before the Delhi High Court and the petition also sought a partial reading down of the confidentiality provision present under Rule 16 of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 issued under Section 69A of the Information Technology Act, 2000.⁴⁰ While the case remains pending before the Delhi High Court, in its written response to the petition, the government has doubled down on its defence of the confidentiality provision and claimed that website owners can be denied access to blocking orders and doing so is necessary to protect the privacy and safety of complainants.⁴¹ However, this does not explain why copies of website blocking orders cannot be shared with website owners after redacting any personally identifiable information of private individuals who may have raised complaints against a website.

The case of Dowry Calculator shows how difficult it can be for website owners and users to find out any information about why a website has been blocked. It is also emblematic of knee jerk and reactionary government censorship which depends on secrecy to survive and targets a wide variety of websites. Based on the 12 instances of government ordered blocking that we studied, we found that websites have been targeted for promoting self-determination or secessionist movements but also for facilitating file transfers and running petition campaigns.⁴² This clearly suggests that website blocking in India is not limited to marginal cases and is increasingly affecting popular mainstream websites as well.

B. Blocking of environmental campaign website, Fridays for Future India

In August 2020, the Environment Ministry received a record breaking 17 lakh submissions in response to the public consultation being held for the Draft Environmental Impact Assessment Notification which many feared would dilute environmental protection standards in India.⁴³ Since the consultation was held during the COVID-19 pandemic, there was limited

⁴⁰ Internet Freedom Foundation, ‘Delhi HC issues notice to government for blocking satirical Dowry Calculator website’ (16 December 2019). Available at: <https://internetfreedom.in/delhi-hc-issues-notice-to-the-government-for-blocking-satirical-dowry-calculator-website/>

⁴¹ Internet Freedom Foundation, ‘MeitY defends blocking of satirical Dowry Calculator website’ (16 March 2020). Available at: <https://internetfreedom.in/meity-defends-blocking-of-satirical-dowry-calculator-website/>

⁴² Database of website blocking orders. Available at: <https://archive.org/details/india-website-blocking-orders-database>

⁴³ Mohana Basu, ‘Modi govt gets over 17 lakh responses to draft EIA’ The Print (13 August 2020). Available at: <https://theprint.in/india/modi-govt-gets-over-17-lakh-responses-to-draft-eia-will-vet-them-to-prepare-final-version/480908/>

scope for physical protests and demonstrations, and digital activism played an integral role in spreading awareness about the erosion of environmental protection standards and facilitating public participation in the consultation process. To make it easier for the public to articulate its objections, volunteer driven environmental groups like Fridays for Future India launched email campaigns which provided the template for an email which could be sent to the Environment Ministry and email IDs of government officials including the Environment Minister. The strategy proved to be too effective and Fridays for Future India's website was suddenly blocked on 10 July in the final month leading up to the deadline for the public consultation.

Fridays for Future was informed by its domain service provider that its website had been blocked pursuant to a notice received from the Delhi Police. Interestingly, the notice issued by the Delhi Police sourced its power from the intermediary liability provision under Section 79 of the Information Technology Act, 2000 instead of relying on the specific website blocking power under Section 69A. However, since Section 79 does not contain a confidentiality requirement like Section 69A, the domain registrar agreed to share a copy of the notice received from the Delhi Police with Fridays for Future. The actual notice issued by the Delhi Police revealed that the Environment Minister had complained about receiving too many emails with the subject line "EIA 2020" and it stated that such unlawful activities could disturb peace and sovereignty of India. To make matters worse, the notice also invoked provisions of the Unlawful Activities Prevention Act, a draconian anti-terror legislation, to direct blocking of the website for containing "*religious hatred content/material*."⁴⁴

In addition to Fridays for Future, other environmental groups such as Let India Breathe and There Is No Planet B also faced blocking of their websites around the same time.⁴⁵ The muzzling of environmental activists and invocation of anti-terror charges led to widespread public outrage. Faced with stiff opposition, the government eventually withdrew the notice directing blocking of Fridays for Future's website and claimed that the invocation of anti-terror charges was an error which had been corrected by issuing new notices.⁴⁶ However, Fridays for Future did not receive any withdrawal order or a new notice and access to the website was silently restored on 24 July 2020.

The blocking of environmental campaign websites demonstrates why focusing solely on Section 69A of the Information Technology Act, 2000 is inadequate even though it is the specialized provision for website blocking under the law. There are a wide range of

⁴⁴ Internet Freedom Foundation, 'Fridays for Future India resists illegal website blocking' (23 July 2020). Available at: <https://internetfreedom.in/fridays-for-future-representation-to-delhi-police/>

⁴⁵ Internet Freedom Foundation, 'We offer our support to environmental activists against web censorship (13 July 2020). Available at: https://internetfreedom.in/blocking_env_web

⁴⁶ Scroll, 'Police use UAPA to block website campaigning against draft environmental rules, later claim error' (23 July 2020). Available at: <https://scroll.in/latest/968367/police-use-uapa-to-block-greta-thunberg-linked-website-campaigning-against-draft-environment-rules>

government authorities - the Ministry of Electronics and Information Technology, the National Internet Exchange of India, state governments, police departments and district magistrates - who are issuing website blocking orders and they are relying on different provisions of law- Section 69A Information Technology Act 2000, Section 79, Information Technology Act 2000, Telecom Suspension Rules 2017, and Section 144, Code of Criminal Procedure 1973. This case study also highlights that ISPs are not the only private entities being directed to block websites and such directions are also being issued to other actors in the ICT ecosystem such as domain service providers.

IV. Lessons and Recommendations for Stakeholders

In this policy brief, we have tried to go beyond the headlines to understand the ground realities of internet censorship in India by focusing on case studies of internet shutdowns and website blocking. Our first set of case studies covered the full spectrum of internet shutdowns ranging from a complete communication shutdown in the border state of Jammu & Kashmir where even landlines were cut off to narrower social media bans in the eastern state of Bihar. Even within individual states, we found that the severity and frequency of internet restrictions can vary significantly. For instance, while it is commonly believed that Jammu & Kashmir is currently experiencing an internet slowdown, we found that in districts like Pulwama, mobile internet services were completely suspended for at least 574 hours or 24 days this year.

In our second set of case studies, we focused on two specific instances of blocking of a satirical website and an environmental campaign website to highlight how procedural safeguards like notice, pre-decisional hearing and issuance of a written reasoned order are often flouted by government authorities to engage in secretive and arbitrary website blocking. Critically, these case studies revealed that website blocking is being ordered against a wide range of websites including popular mainstream websites and it is being implemented by different private entities in the ICT ecosystem including ISPs and domain service providers.

We decided to study internet shutdowns and website blocking together because they fall on different ends of the same spectrum of internet restrictions. Further, incidents like social media bans being ordered in Bihar under the Telecom Suspension Rules, which were meant to authorize conventional internet shutdowns, clearly indicated that these problems cannot be understood in silos. Finally, internet shutdowns and website blocking both raise similar concerns about transparency, accountability, vagueness, availability of less restrictive alternatives and exercise of these powers by unauthorized officials.

In this final section of the policy brief, we have drawn on the case studies to identify useful lessons for different stakeholders and to develop recommendations which can be implemented to mitigate the harm caused by internet censorship in India.

A. For Lawyers

(i) Collaboration

Lawyers commonly rely on legal authorities like legislations and case law to prove their client's case. However, this may not be enough for litigation related to internet censorship which often involves complex technical issues that may be beyond the understanding of many judges. For instance, if a court is expected to determine if 2G speed constitutes effective internet access in 2020, technical evidence must be produced which clearly demonstrates the impact of 2G v. 4G on web performance. Similarly, to explain the importance of the internet as essential infrastructure which facilitates not merely speech but also access to healthcare, education, trade and business, it is vital to produce testimonies of actual people affected by internet restrictions and the losses suffered by them. For this purpose, lawyers working on cases challenging internet restrictions must collaborate with technologists, economists, journalists and local activists to ensure that the harm caused by internet restrictions is undeniably proven before a court. This is particularly important because government authorities routinely deny any adverse impact of internet restrictions, and unless concrete facts and figures are produced to challenge this narrative, courts may accept the government's claims at face value.

(ii) Incrementalism and Iteration

As we saw in the case of *Anuradha Bhasin v. Union of India*, litigation challenging internet restrictions may not provide immediate substantive relief since court cases can drag on for a long time and judges may be reluctant to intervene if national security interests are invoked by the government. However, even in such circumstances, incremental improvement in the status quo is possible and the threat of litigation can also nudge government authorities to at least comply with the letter of the law, if not its spirit. This kind of incrementalism when combined with strategically planned future interventions can provide meaningful relief to people affected by internet shutdowns and website blocking. For instance, while much remains to be done, 4G mobile internet was finally restored in at least 2 out of 20 districts of Jammu & Kashmir on 16 August 2020 after three successive rounds of litigation before the Supreme Court.⁴⁷

B. For Civil Society Organizations

(i) Measurement

As we found through the case studies, it can be difficult for people to determine if online content is inaccessible because of government ordered restrictions or due to technical errors. This problem is particularly acute in the context of website blocking which is inconsistently implemented and recent research suggests that only 27.64% of blocked websites are

⁴⁷ Internet Freedom Foundation, 'Govt agrees to staggered restoration of 4G mobile internet in J&K before Supreme Court' (11 August 2020). Available at: <https://internetfreedom.in/staggered-4g-restoration-j-k/>

uniformly blocked by all six major Indian ISPs.⁴⁸ In these circumstances, the development and use of measurement tools is necessary to get an accurate and complete picture of internet censorship in India. Fortunately, efforts are already being made in this direction, and researchers have used the Open Observatory of Network Testing (OONI) probe to test and compare website blocking in different states of India⁴⁹ and to develop their own measurement tools.⁵⁰

(II) Government engagement

Our case studies revealed that in many instances, internet restrictions were ordered by government officials in response to credible threats of large-scale violence along the lines of religion or caste. India has witnessed several devastating communal riots since it became an independent country in 1947 which have left thousands dead or displaced. Therefore, the concerns of local government officials who are expected to control violent and unruly mobs cannot be dismissed lightly. It is necessary for civil society organizations to engage with government officials to explain how internet restrictions can actually incentivize violent protests which require less communication and coordination than peaceful demonstrations. It is also important to work with government officials to highlight how technology can be used to diffuse tensions by debunking rumours and providing accurate information. Finally, there is need for more empirical research about both positive and negative use of the internet during communal riots in different parts of India since the role played by the internet in documentation of atrocities and fact checking cannot be ignored.

C. For ICT Companies

(I) Mitigation

Our conversation with an ISP revealed that due to onerous license conditions and harsh penalties, companies do not have much scope to push back against government requests. The interviewee stated that even if what was being sought by the government was practically infeasible, ISPs would still confirm compliance because as they vividly put it: *“The license conditions make the Department of Telecommunications a God-like figure for ISPs.”* The companies also fear that they may not receive protection from the judicial branch if they challenge the government’s actions because recently, the Indian Supreme Court has come down very severely on the telecom industry by interpreting existing legal provisions in a manner that poses an existential threat to these companies by requiring them to pay huge sums of money within a short period of time.⁵¹

⁴⁸ Supra note 9

⁴⁹ Chinmayi SK, ‘Those Unspoken Thoughts: A study of censorship and media freedom in Manipur, India’ Open Technology Fund (June 2020) Available at: <https://ooni.org/documents/those-unspoken-thoughts-otf-fellow.pdf>

⁵⁰ Centre for Internet & Society, Censor Watch. Available at: <https://cis-india.github.io/censorwatch/index.html>

⁵¹ Shreyashi Roy, ‘SC gives telecoms 10 years to pay dues: 15 year long AGR case, explained’ The Quint (03 September 2020). Available at: <https://www.thequint.com/explainers/agr-case-bharti-airtel-jio-vodafone-idea-department-of-telecommunications-supreme-court-case>

Even in democratic countries like India, certain regions may be unusually difficult to operate in due to geo-political reasons. For instance, in Jammu & Kashmir, telecom service providers have to comply with additional customer verification requirements for pre-paid subscribers and unless these requirements are fulfilled, pre-paid subscribers cannot be allowed even 2G mobile internet access. While operating in such regions, it is very important for companies to be sensitive to hardships being experienced by the local population and to provide them appropriate concessions. For instance, when voice call services were restored in Jammu & Kashmir in October 2019, Airtel, which has the largest subscriber base in Jammu & Kashmir, agreed to waive off post-paid rental charges for the period during which these services were suspended by the government.

Despite these limitations associated with operating in a hostile legal regime, there are still some ways in which ICT companies can mitigate the adverse impact of internet restrictions. As we saw in the case studies, in many cases, government officials want to narrow the scope of internet shutdowns but they may not have the technical knowledge and ability to do so. For instance, in Rajasthan, the internet shutdown orders issued to prevent cheating in police constable recruitment exams only required suspension of internet services in and around examination centres. Similarly, while imposing social media bans, the orders issued by the Bihar government clarified that only new uploads had to be blocked on YouTube and there was no prohibition on people watching existing videos. In such cases, good faith engagement may be possible between ICT companies and government officials to develop solutions which ensure the scope of internet restrictions is limited to what is actually required.

(II) Learning

Indian ICT companies would benefit from learning about international best practices adopted by their foreign counter-parts. Here, it may be instructive for them to refer to the GNI Implementation Guidelines which provide practical and detailed guidance on how companies can fulfil their human rights obligations.⁵² The GNI Independent Assessment Reports which include case studies describing how different companies have handled government demands could also serve as a useful learning resource.⁵³ Based on these case studies, David Sullivan has distilled five specific recommendations for companies facing government ordered network disruptions which include seeking clarity about legal obligations, documenting and

⁵² Global Network Initiative, Implementation Guidelines for The Principles on Freedom of Expression and Privacy. Available at: <https://globalnetworkinitiative.org/wp-content/uploads/2018/08/Implementation-Guidelines-for-the-GNI-Principles.pdf>

⁵³ Global Network Initiative, Independent Company Assessment Reports. Available at: <https://globalnetworkinitiative.org/company-assessments/>

escalating all demands, narrowing the scope of disruptions, increasing transparency and collaborating with other stakeholders.⁵⁴

If these recommendations are put into practice by Indian ICT companies, it would significantly improve the status quo. In particular, companies should at least be more transparent in their operations and inform users if they have been subjected to government ordered censorship. As we previously noted, many people may not be able to determine why a website is inaccessible or why internet services seem slow. Here, ICT companies could step in to provide their users information about which government authority has directed service disruption, under which legal provision, and for what period of time. Having this kind of information about government ordered censorship will also make it easier for aggrieved individuals to promptly challenge such measures before courts, especially if the order is issued under an incorrect legal provision or by an unauthorized government official.

(III) Circumvention

ICT companies which develop circumvention tools such as VPNs should consider the needs of users in countries where threats exist outside a rule of law framework. For instance, bans on VPNs in Jammu & Kashmir have been enforced through physical violence and people have been assaulted by police officials if VPN apps were found on their phone during random searches at highway checkpoints and other public spaces.⁵⁵ Therefore, while developing and designing their products, companies should consider the risks faced by users living in regions where human rights violations are common and offer discreetly named or designed alternatives which may stand a better chance at avoiding detection during such random searches.

In conclusion, addressing internet shutdowns and website blocking in India will require cooperation and collaboration between different stakeholders who all have a role to play at different stages of the cycle of Internet censorship. Transparency by ICT companies will facilitate strategic litigation by lawyers and research by civil society groups. The outcome of such litigation and research must then be communicated to government officials to ensure compliance with judicial directions and evidence-based decision-making respectively.

⁵⁴ David Sullivan, 'Five Ways Telecommunication Companies Can Fight Internet Shutdowns' Lawfare (23 August 2020). Available at: <https://www.lawfareblog.com/five-ways-telecommunications-companies-can-fight-internet-shutdowns>

⁵⁵ Shoaib Mir, 'As J&K Police Probe VPN Use, Kashmiris 'Forced' to Allow Smartphone Checks' The Wire (25 February 2020). Available at: <https://thewire.in/tech/kashmir-police-vpn-smartphone-checking>